

BUILD INVISIBLE NETWORKS

We **cloak** your private
network from
vulnerabilities

Invisible Internet™



Preface

Hackers can't hack what they can't see. Our invisibility cloak represents a whole new paradigm to infrastructure protection beyond Zero Trust by taking remote communications "off the grid" while preserving the existing infrastructure and development investments.

NVIS is military-grade security built by the team that created a best-in-class unhackable solution approved for DoD-wide use and for Coalition forces.

NVIS is revolutionary in the security and privacy space to benefit B2B or B2G greatly, especially in the global threat climate.

Connect to anyone in the world,
securely without restrictions

NVIS Can't be

- Hacked
- Sniffed
- Traced
- Blocked
- Censored

Cost Effective: Take advantage of existing networks or
public infrastructure



Who We Are



Phil Smith

Founder / CTO

- Founder/creator and chief architect
- Expertise in security, networking, ISP and blockchain.
- Over 30 years in lead roles at NASA, HP, Cisco, Lawrence Livermore National Lab



Marilyn Hernandez

Co-Founder

- Investor relations, Business Development, Sales and Marketing, Strategist, Researcher, Realtor, Counselor,
- BA Administration of Justice



Salman Rizvi

CEO – (CMO/CRO)

- 22+ years Leadership of Enterprise Transformation for the top Fortune 50-500 and organizations worldwide
- Founded 2 companies
- SaaS pipelines, CIO, EVP & Strategic Advisor



Jed Reitler

SVP Sales & Marketing

- 15+ years of experience in Sales, Marketing, Strategy
- Founded 3 companies
- 5 years of consulting for tech startups
- Mentor for tech founders at Stanford and Skolkovo



Rob Langhorne

CISO

- Former CEO of CloudLogix, Cranite architect, Apple lead
- Analytical, highly adaptable professional
- Extensive experience leading ground-breaking development in mobile computing and security.



LINKSYS



opentext™

Our Advisors



Dr. Taher Elgamal

CTO / Security, Salesforce

- Dr. Elgamal is world renown in the industry as **the inventor of Secure Sockets Layer (SSL)**, a protocol developed by Netscape for transmitting private documents via the Internet. Dr. Elgamal also wrote the **SSL patent and promoted SSL and has a lifetime achievement award from RSA.**



John Vigouroux

Chief Entrepreneur & Innovation Officer, Averett University

- CEO & Co-Founder at WeRAI
- Former CEO Nex Cubed
- CEO of Cranite Systems
- CEO of M86 Security, (acquired by Trustwave) joined as an advisor.



Manoj Bhatia

Partner Business Development, Verizon

- Formerly Worldwide Sales and Business Development Leader Cisco Systems
- Director Smart Grid Strategic Alliances, GE Digital Energy



Gregory F. Ryan

President, Ryan Advisory Services

- Providing Business Consulting
- Management Consulting
- Finance Consulting
- Marketing Consulting
- Pricing Strategy
- Advertising
- Project Management

The Core Problem

VISIBILITY IS THE PROBLEM

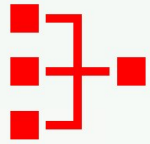
Internet is OPEN which means **VULNERABLE BY DESIGN**:

- Geolocation
- Routes are traceable
- Lookup by name (DNS)
- IP address is public
- TCP ports well known / discoverable
- Open Protocols yield Connectivity but NO SECURITY

Result: Global Cost of Cybercrime 10.5 Trillion dollars Annually*

* Projected by CyberSecurity Ventures, 2021

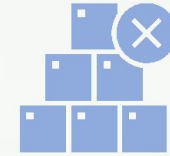
Problems



Single Point of Failure



Slow Performance



Lack Scalability



High TCO



Lack of Privacy



Highly Vulnerable

Solutions



Decentralized



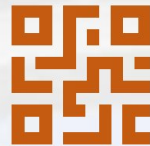
High Performance



Infinite Scalability



Easy to Deploy



Encrypted End-to-End



Invisible

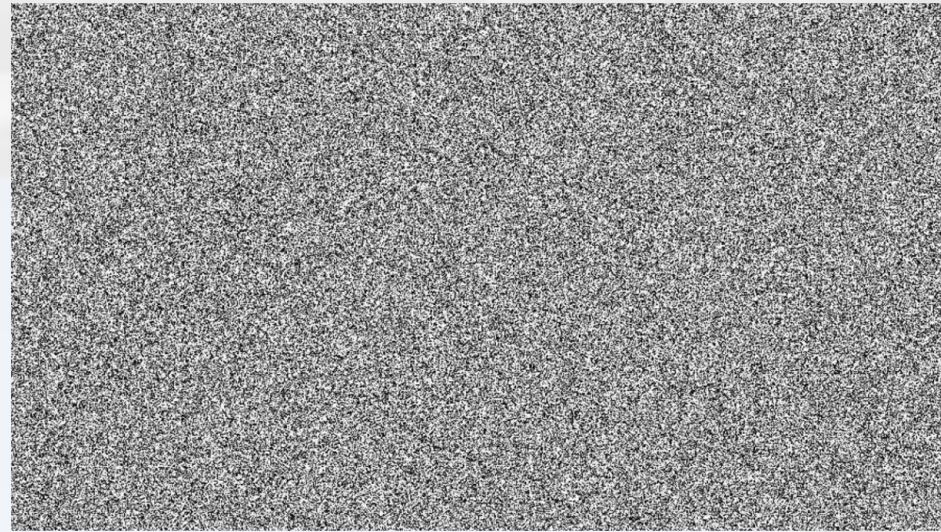
Innovation: Layer 2 Full Stack Security

- A Software-Only Architecture
- Layer2 Encryption
 - Layer 2 encrypts ALL traffic including source, destination and data payload so the full stack is secured.
 - Only software based Layer 2 product obtaining FIPS certification
 - No IP routing (hops) needed boosting performance by removing overhead and propagation delays.
- Protects against the following
 - Access Point / MAC address spoofing
 - Dictionary attacks
 - Man-in-the-middle
 - DDOS attacks
 - ARP connection/redirection
 - Protocol hacks – ALL OF THEM

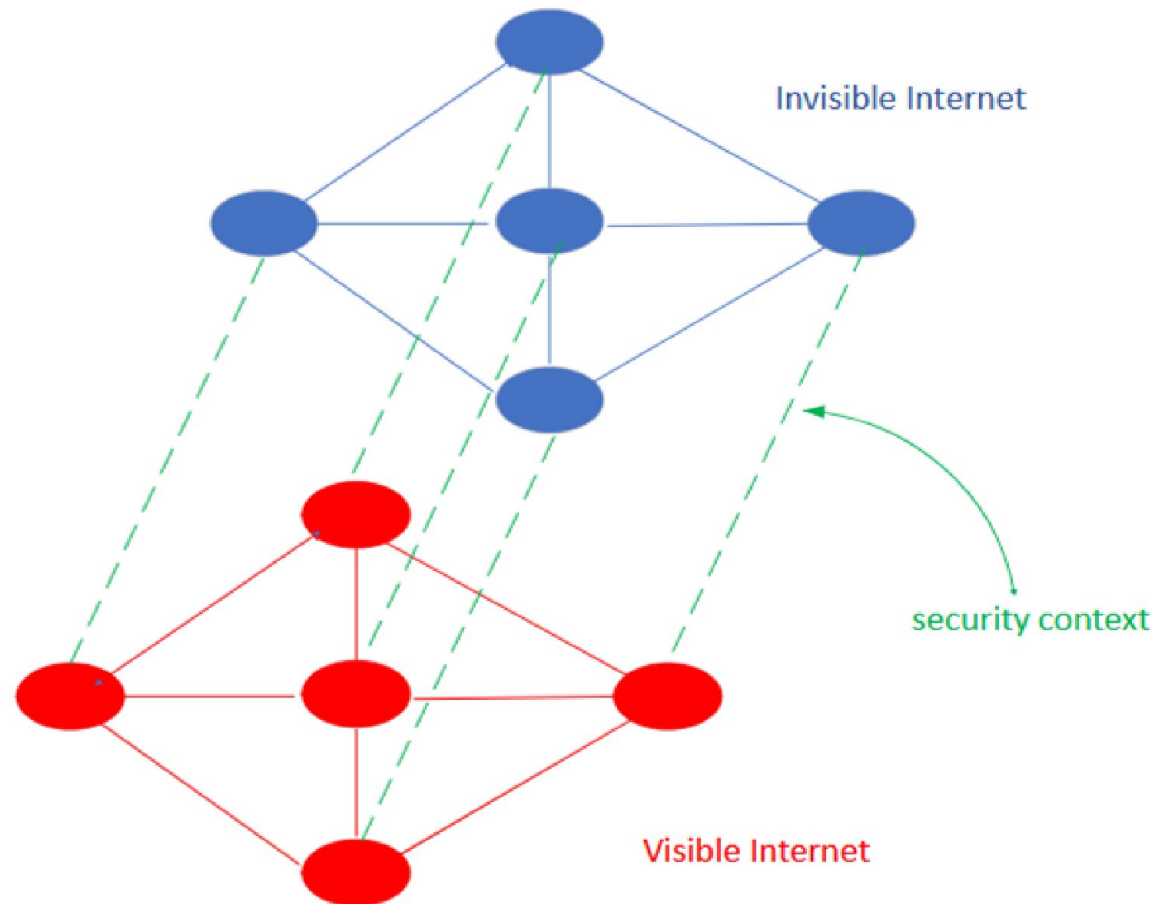
#	ISO/OSI Model	Example
7	Application	HTTP, FTP
6	Presentation	SSL, TLS
5	Session	NetBIOS, PPTP
4	Transport	TCP, UDP
3	Network	IP, ICMP
2	Data Link	NVIS over Ethernet, WiFi, WiMAX, LTE
1	Physical	Copper Wires, Optical Fibers, Air

Innovation: Peer-to-Peer Path Invisibility

Perimeter Path and Payload Encryption
Turns This



Innovation: Mirrored Segments



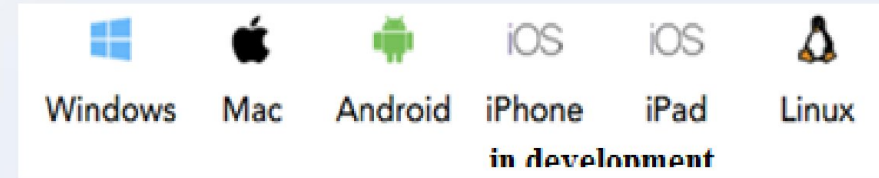
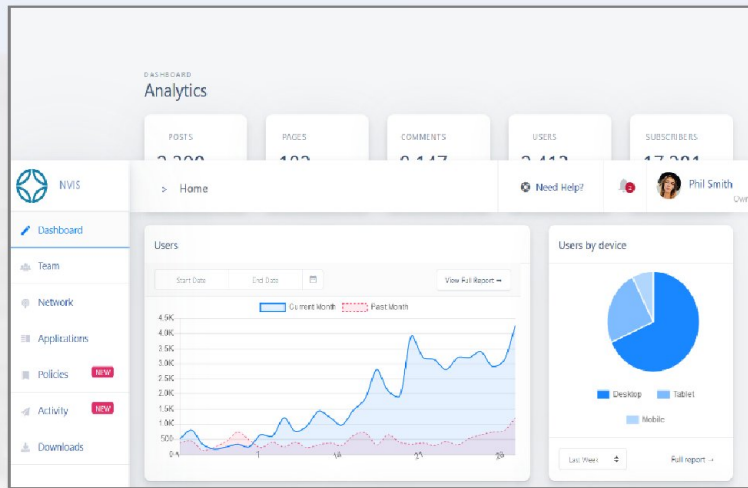
Patent Pending: A
Multiverse of
Internets, 2019,
A. Smith EFS ID
3483382

Virtual Private IPs
behaves like Public
IPs – no gateways or
routing needed.

Multiple overlays can
segment networks
by security context.

Product Description

Admin Web UI



- 100% software agents – **no hardware needed ****
- All major platforms for end-users
- AWS and Azure Cloud Supported
- Web Subscription and Billing System

** ARM router available for Kiosk. legacy systems or IoT connectivity

Admin Web UI

1

Add Group

Group name

Group PSK

2

Add New Member

Member name

Member Email Id

Address

IP

Group

One click auto provisioning

3

Add New Computer

Host

Address

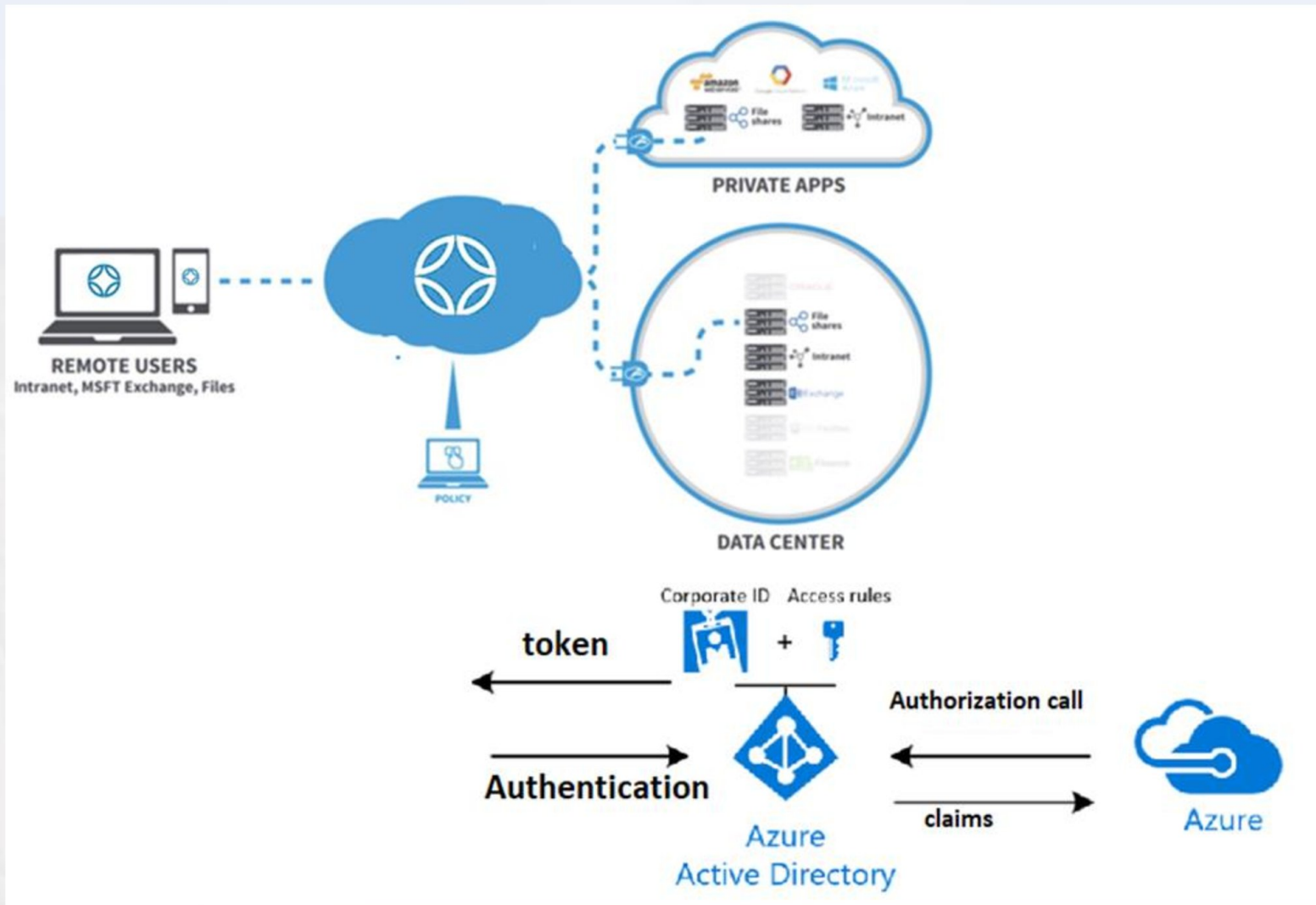
IP

Group



Build a network as easy as 1-2-3

System Level View - Zero Trust



The Market

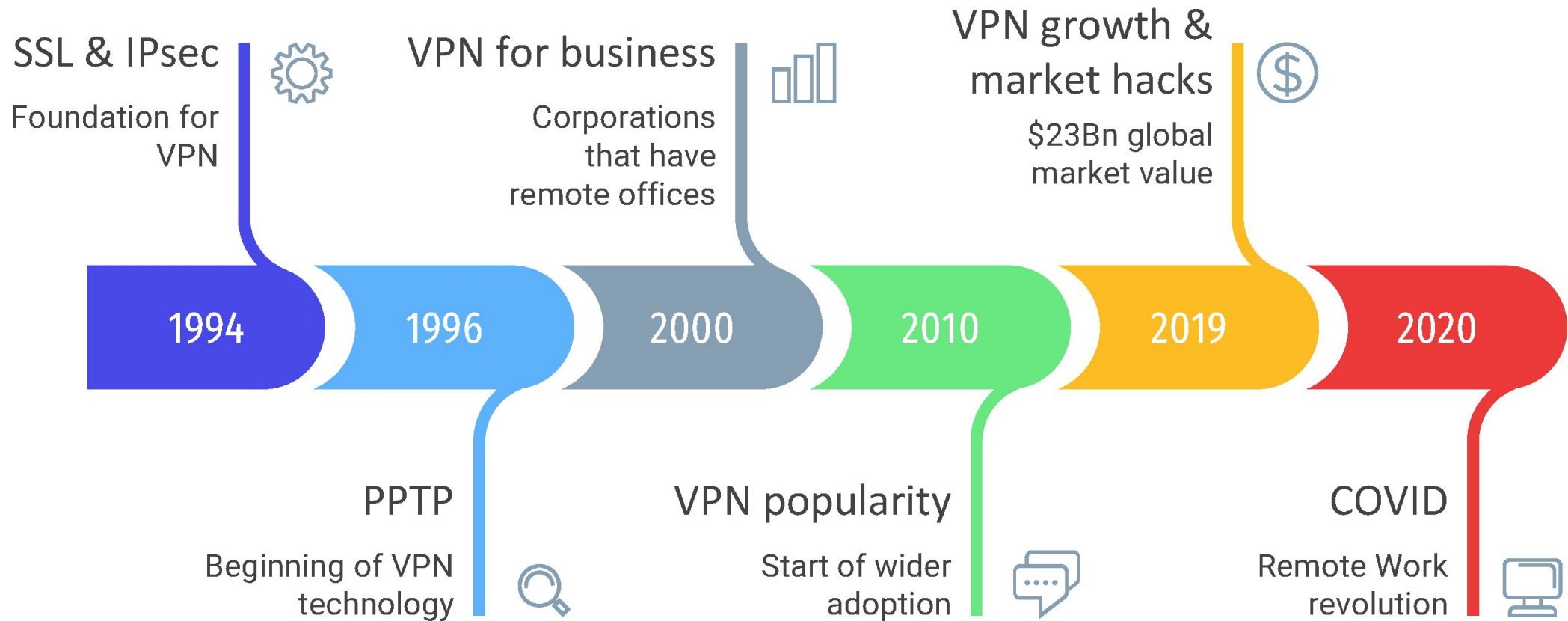
“

VPN Hacks Are a Slow-Motion Disaster

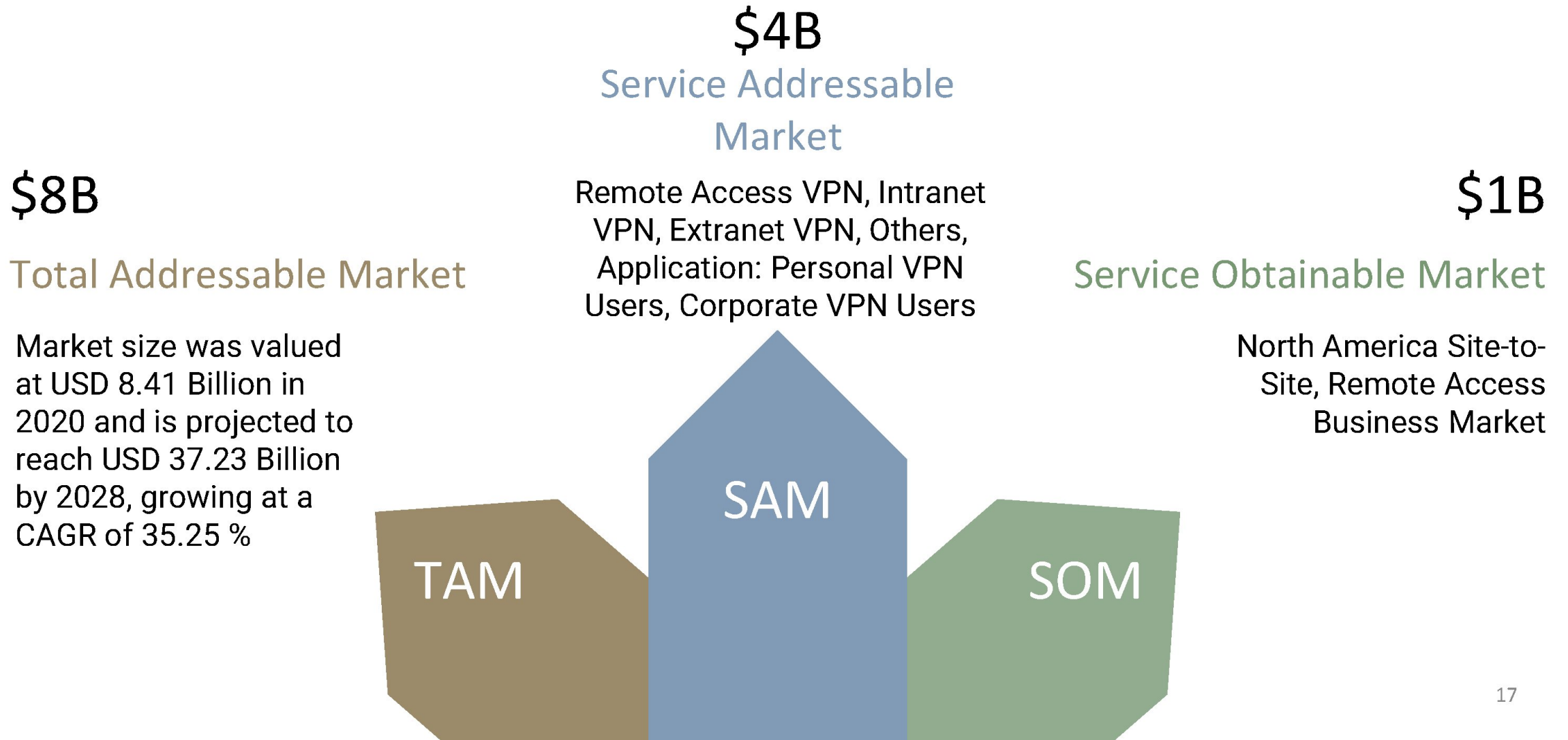
Hackers have had a field day with virtual private networks — especially during the remote-work pandemic era.

WIRED

Why Now – Existing Security is Flawed



The Market



Securing the Hybrid Workplace in 2022



94%

companies are concerned about the security of corporate data exposed via home-based devices



74%

expect more use of BYOD, and an increased need for device authorization



40%

expect half of their workforce will work remotely at least twice a week

Zero Trust Adoption Report, conducted by Cybersecurity Insiders, found that 15 percent of organizations have already enacted ZTNA while **more than half (59%) plan to implement ZTNA** over the course of the next 12 months

3/10

are protected against VPN attacks which cybercriminals are now taking advantage of to impact business operations

Business Model

ENTERPRISE LICENSING

- Subscription Licensing
- Network Access or Use
- OEM Licensing

MANAGED SERVICES

- Customized or private server setup

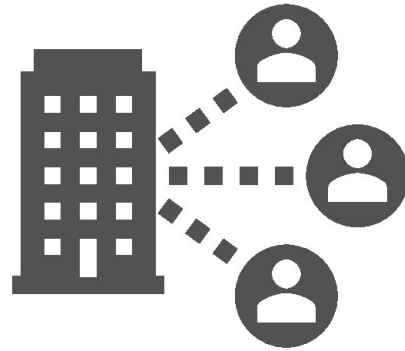
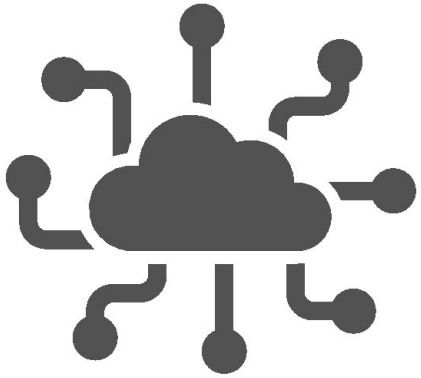
MOBILE LICENSING

- Monetized client apps

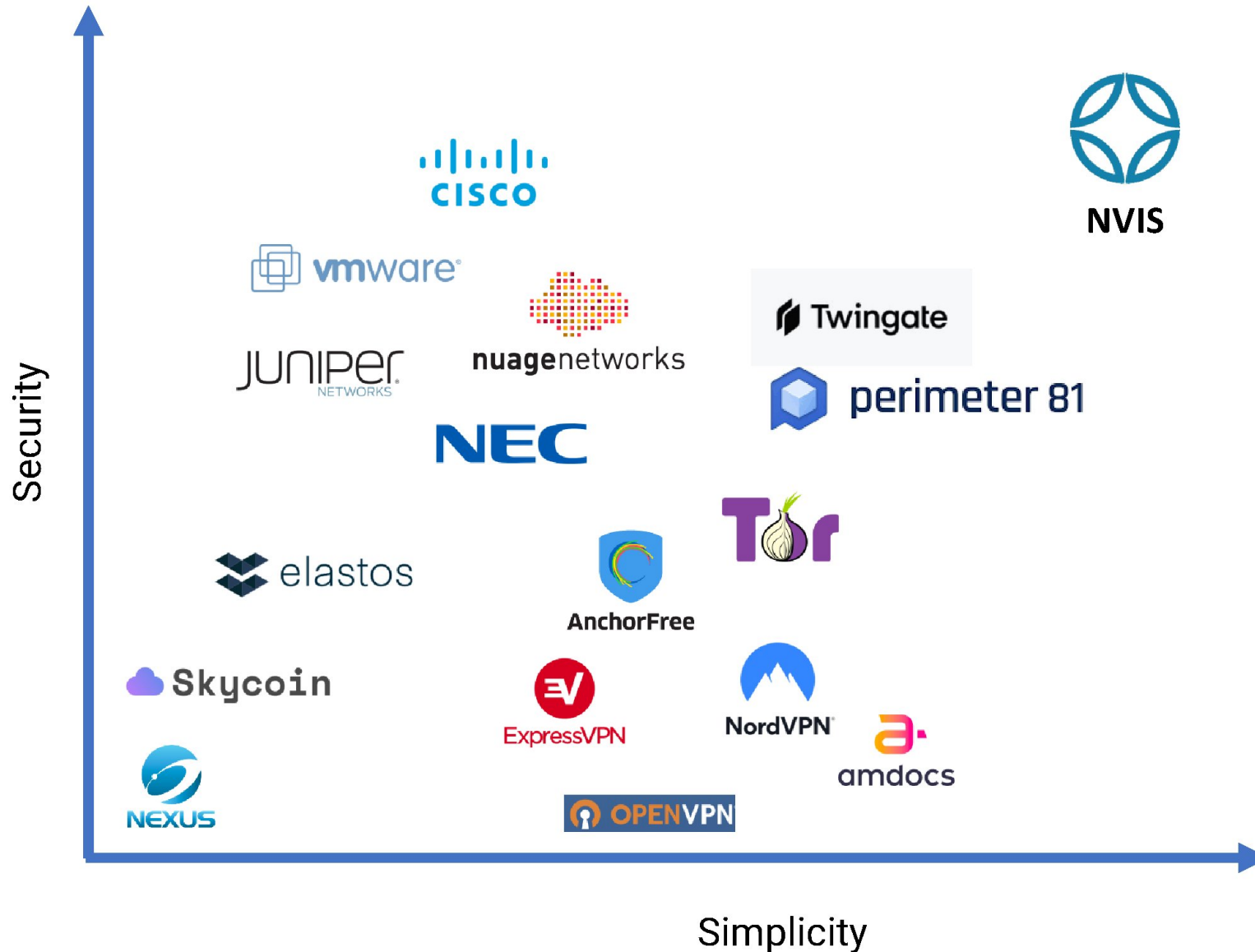
CONSULTING SERVICES

- Professional Services for planning and integration

Disruptive, SaaS and Headless



Competitive Position



Differentiators

- Zero Trust / MFA
- Software Defined Perimeter
- Invisible to any outside attack
- Layer 2 Networking
- End-to-End Encryption
- Peer-to-Peer Architecture
- High Performance & Scalable
- Configure & Deploy in Seconds
- Private Static IPs over Internet
- Untraceable & Unblockable
- Multiplatform Support
- Enterprise Grade/SMB Priced
- No Tracking or Data Selling
- No Split Tunneling Required
- No Special OS Required
- No Special Hardware Required
- No Network Expertise Required
- No Security Expertise Required

Customer Acquisition Strategy



Launch

SEO
Reddit
Twitter
LinkedIn
Reviews/Bloggers
MSP Partnerships
Cloud Partnerships

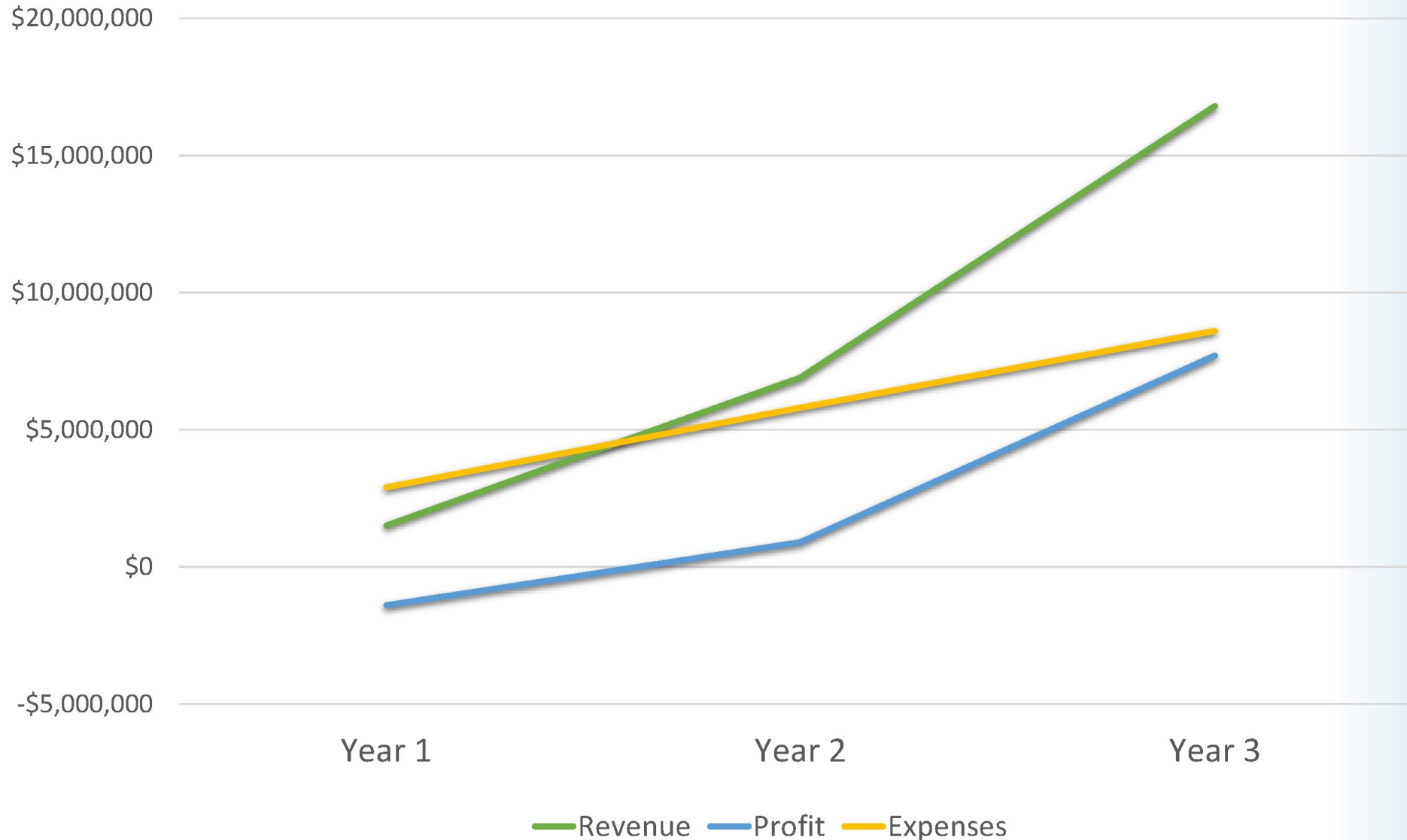


Scale

Events
Conferences
Sponsorships
Affiliate Programs
Direct Salesforce
PPC Campaigns
YouTube Channel

Financial Projections

Revenue estimate in first 3 years after funding



KEY ANALYSIS

- \$16M Revenue in 3yrs
- \$7.7M Profit in 3yrs
- Positive Cash Flow in 6 months
- **Break Even in 18 months**
- Average Sale per B2B Client \$627 annually
- Enterprise up to \$600K each

The Ask

**\$2 Million
in Seed
Investment**

**SAFE note
\$8 Million
Pre-Money**

**Break Even
Goal
18 months**

To hit fast growth, we will allocate the money to:

Core development - 32%
Operational - 22%
Marketing & Sales - 39%
Legal and compliance - 7%

Exit Strategy

- Network equipment manufacturers (Cisco, Juniper)
- Cloud providers (AWS, Microsoft, Google, IBM)
- Security or VPN companies
- Banks (or interbank service providers)
- Platform tech companies (Google, Microsoft, etc.)
- Telco or utility companies (or inter-company communication providers)
- Facebook or other social media giant (with current emphasis on privacy)



Phil Smith
Founder | NVIS Inc.



phil@nvis.me



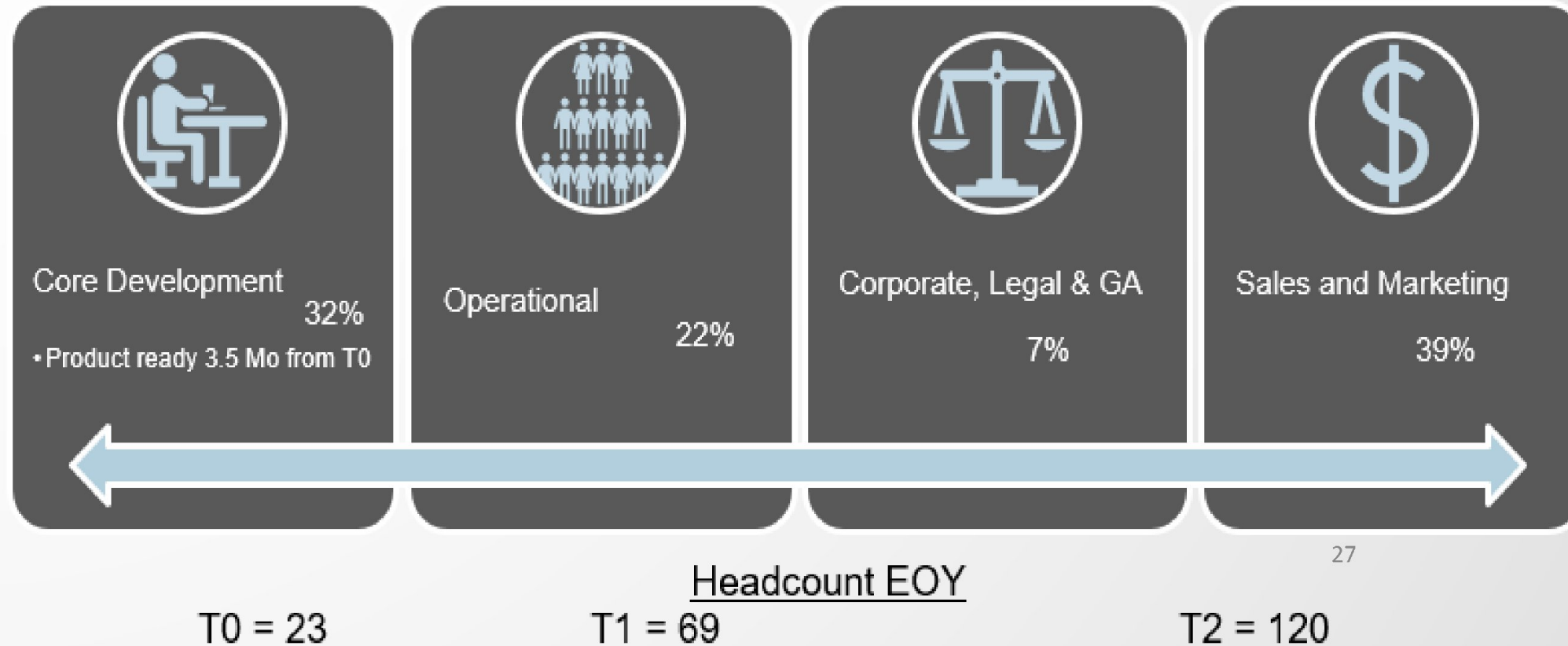
1.408.400.3256

Thank You

Backup

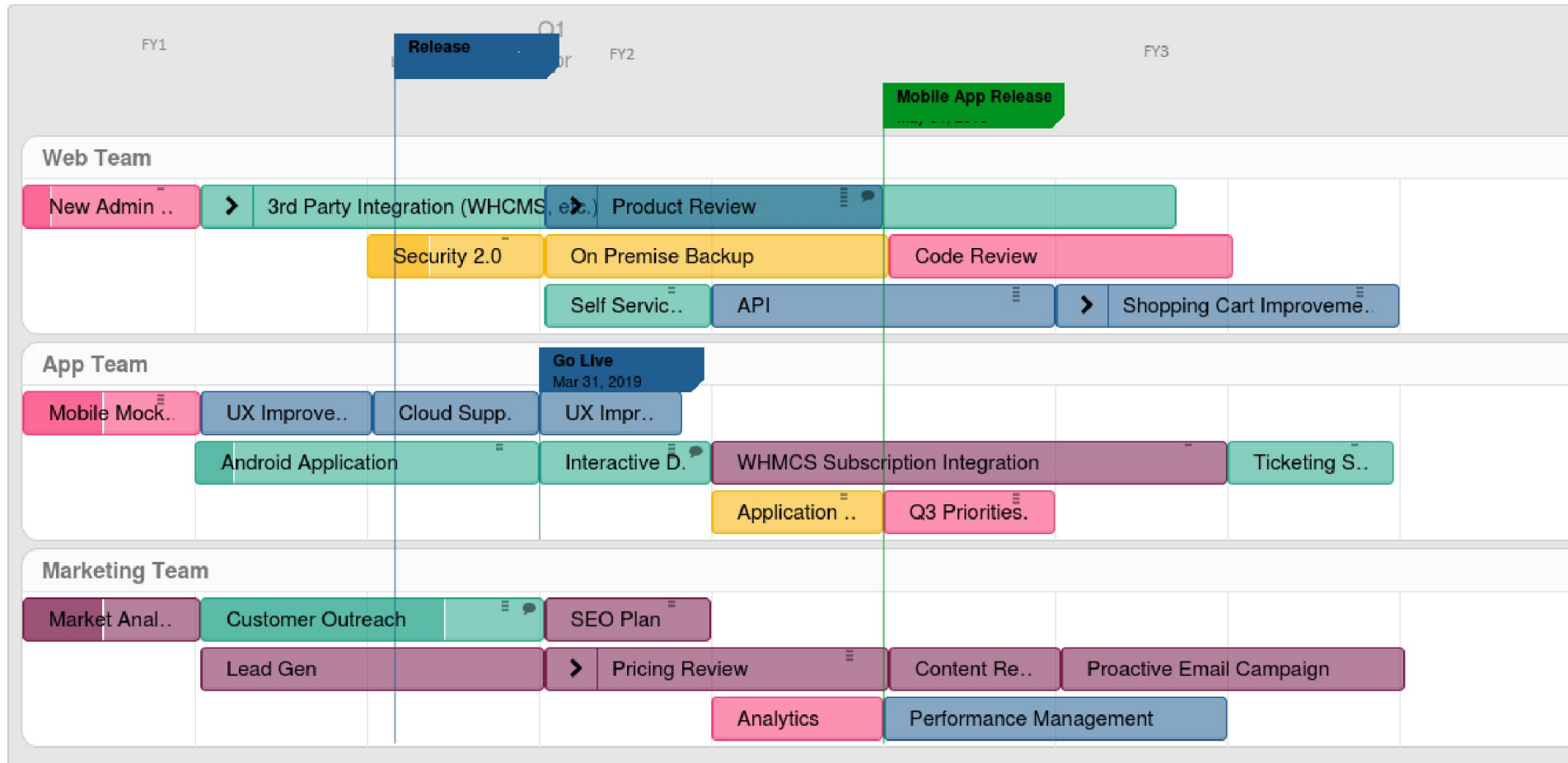
Slides

GO TO MARKET: USE OF FUNDS



Roadmap

NVIS Product Roadmap



Strategic Goals

- Enhance Performance
- Increase Customer Satisfaction
- Increase Revenue
- Internal Optimization
- Security Improvements

SaaS Subscription


		Monthly	Annually**
Business Bundles	#Nodes* (up to)	\$6/Node	\$5/Node
5-Pack	5	\$ 30	300
10-Pack	10	\$ 60	600
25-Pack	25	\$ 150	1500
Enterprise Bundles		\$11/Node	\$10/Node
50-Pack	50	\$ 550	6000
100-Pack	100	\$ 1,100	12000
250-Pack	250	\$ 2,750	30000
250+	Unlimited	Custom	Custom

* Node = Clients, Endpoints, Gateways

** Annually = 12 Month Pre-paid subscription

Features, Security & Cost Comparison

COMPETITIVE ANALYSIS

	CENTRALIZED VPN	TOR NETWORK	
Port Cloaking	No	No	Yes
Decentralized Traffic Routing	No	Yes	Yes
Possibility for end to-end protection	No	Yes	Yes
Spoofing Risk	High	Low	Low
Network Participants Incentivized	No	No	Yes
Open Source	No	Yes	Yes
Speed	High	Low	High/Medium
Platform as a Service	No	No	Yes
Named Groups	No	No	Yes

Bundle	NVIS	TORguard	OpenVPN	Perimeter 81
Starter	\$25	\$69	\$41	\$40
Standard	\$50	\$110	\$58	\$80
Medium	\$100	\$169	\$117	\$200
Enterprise	\$500	Custom	\$175	\$400
Enterprise+	\$1,000	Custom	\$233	\$800
Enterprise++	\$2,500	Custom	\$467	\$2,000

**Subscription charges per client per month basis.

Traction

- **MVP** test network over 1 year continuous operation with invisible blockchain nodes intercommunicating in Paris, Amsterdam, US, Canada, Tokyo and Singapore.
- **Verified** connections from Beijing, Moscow, Saudi Arabia and other locations where Internet and VPNs are censored or blocked
- **MOU with HowDoo.io**, social media
- **MOU with FYRM**, a penetration test and security company to validate NVIS
- Core technology **tested** by [Miercom Labs](#). Ranked **most secure**, invulnerable to attacks, where Ipsec and SSL VPNs all fail.



Partners and Resources



Amazon



Cisco



HP



Vultr Hosting



McAfee

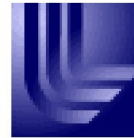


CloudDNS

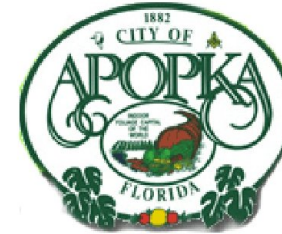


Upserve

Legacy Customers



Lawrence Livermore
National Laboratory



U.S. Army Inspector
General School

